UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/609,323	06/27/2003	Surendra N. Naidoo	4017-02806	7354

30652 7590 12/06/2005

CONLEY ROSE, P.C.
5700 GRANITE PARKWAY, SUITE 330
PLANO, TX 75024

EXAMINER	
RAMAKRISHNAIAH, MELUR	
ART UNIT	PAPER NUMBER
2643	

DATE MAILED: 12/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/609,323	NAIDOO ET AL.	
	Examiner	Art Unit	
	Melur Ramakrishnaiah	2643	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *23-25,29-31,53 and 58-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *23-25,29-31 and 58-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10-06-2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 23-24, 29-31, 53, 58, are rejected under 35 U.S.C. 103(a) as being unpatentable over Nabavi (GB 2325548) in view of Nadooshan (US PAT: 6,161,182), Katz (US PAT: 5,412,708).

Regarding claim 23, Nabavi discloses a method for remote monitoring of premises, the method comprising: operatively coupling a remote client (9, fig. 1) to a security system server (10, fig. 1) being capable of authenticating a user of the remote station, operatively coupling the remote client to a security gateway (reads on 1, fig. 1), the security gateway being capable of managing the monitoring of one or more portions of the premises, transferring information between the security gateway (1, fig. 1) and the remote client (9, fig. 1), wherein the user is at a location, which is geographically remote from the premises, wherein access to the security gateway by the remote client is allowed based upon the access permissions for the user (figs. 1-3, page 6, line 3 to page 7, line 22).

Regarding claim 58, Nabavi discloses a security system for remote monitoring of a premises by a user of a remote client, the security system comprising: a security gateway (reads on 1, fig. 1) coupled to the security system server (reads on 10, fig. 1) via the network (7, fig. 1), the security being capable of managing the monitoring of one

or more portions of the premises, one or more cameras (6, fig. 1) located at the premises to the security gateway, one or more audio stations located and operatively coupled to the security gateway, where the user at a location which is geographically remote from the premises (figs. 1-3, page 6, line 3 to page 7, line 28).

Nabavi differs from claims 23 and 58 in that he does not teach the following: verifying the identity of the user of the remote client, transmitting authorization information from the security system server to the remote client and from the security system server to the security gateway, the authorization information transmitted to the remote client including access permissions for the user, the remote client using the authorization information to operatively couple the security gateway, remote client cannot access directly the security gateway without the information provided, to the remote client, by the security system server, wherein the security system server provides the remote client with authorization information, access permissions based upon a permission profile created by a general administrator of the security gateway, activating a signal at the premises for notifying an occupant at the premises that remote monitoring is occurring.

However, Nadooshan teaches the following: verifying the identity of the user of the remote client, transmitting authorization information from the security system server to the remote client and from the security system server to the security gateway, the authorization information transmitted to the remote client including access permissions for the user, the remote client using the authorization information to operatively couple the security gateway, remote client cannot access directly the security gateway without

the information provided, to the remote client, by the security system server, wherein the security system server provides the remote client with authorization information (figs, 1, 9, col. 9, line 48 – col. 8, line 14), access permissions based upon a permission profile created by a general administrator of the security gateway (this is implied as illustrated in figs. 5-6, col. 6 lines 29-58); Katz teaches the following: activating a signal at the premises for notifying an occupant at the premises that remote monitoring is occurring (col. 10 lines 46-58).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify Nabavi's system to provide for the following: verifying the identity of the user of the remote client, transmitting authorization information from the security system server to the remote client and from the security system server to the security gateway, the authorization information transmitted to the remote client including access permissions for the user, the remote client using the authorization information to operatively couple the security gateway, remote client cannot access directly the security gateway without the information provided, to the remote client, by the security system server, wherein the security system server provides the remote client with authorization information, access permissions based upon a permission profile created by a general administrator of the security gateway as this arrangement would provide means for centralized control of security access to the remote premises, thereby enabling central control of all access to the remote systems as taught by Nadooshan; activating a signal at the premises for notifying an occupant at the premises that remote monitoring is occurring as this arrangement would provide initial notification to the

affected users of the system who are being video recorded so that any privacy concerns are addressed before commencement of recording as taught by Kastz.

Claim 53 is similar to claim 23 and is rejected for the same reasons as set forth in the rejection of claim 23.

Regarding claims 24, 29-31, Nabavi does not teach the following: general administrator of the security system is capable of modifying the user permission profile, permission profile for the user identifies specific features of the security gateway which may be accessed by the remote client, access permission enables the user to access one or more designated cameras located at the premises, the access permissions for the user enables the user to access one or more designated audio stations located at the premises.

However, Nadooshan teaches the following: general administrator of the security system is capable of modifying the user permission profile (this is implied in as much as the reference teaches establishing profile for each user as shown in figs. 5-6), permission profile for the user identifies specific features (reads on login level for each user) of the security gateway which may be accessed by the remote client, access permission enables the user to access one or more designated cameras (reads on login level permitted for each user with respect to each equipment) located at the premises, the access permissions for the user enables the user to access one or more designated audio stations (reads on login level permitted for each user with respect to each equipment)located at the premises (figs. 5-6, col. 6 lines 29-58).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify Nabavi's system to provide for the following: general administrator of the security system is capable of modifying the user permission profile, permission profile for the user identifies specific features of the security gateway which may be accessed by the remote client, access permission enables the user to access one or more designated cameras located at the premises, the access permissions for the user enables the user to access one or more designated audio stations located at the premises as this arrangement would facilitate to set up user access to different equipments and its features by setting up user login levels as taught by Nadooshan, thus satisfying different security needs required for given application.

3. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nabavi in view of Nadooshan as applied to claim 23 above, and further in view of Gullman et al. (US PAT: 5,280,527, hereinafter Gullman).

Regarding claim 25, the combination does not teach the following: step of verifying the identification of the user comprises authenticating biometric data.

However, Gullman teaches the following: step of verifying the identification of the user comprises authenticating biometric data (col. 2 lines 28-39).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: step of verifying the identification of the user comprises authenticating biometric data as this arrangement would facilitate authenticating the user by another well known means as taught by Gullman, thus providing another alternative to verify user authenticity.

4. Claim 59 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nabavi in view of Horii et al. (JP363033088A, hereinafter Horii), Nadooshan and Lemons et al. (US PAT: 6,504,479, filed 9-7-2000, hereinafter Lemons).

Regarding claim 59, Nabavi discloses a security system for remote monitoring of a premises by a user of a remote client, the security system comprising: a security system server (reads on 10, fig. 1), the security system server being capable of authenticating the user of remote client (9, fig. 1), a security gateway (reads on 1, fig. 1) operatively coupled to the security system server via a network (7, fig. 1), the security gateway being capable of managing the monitoring of one or more portions of the premises, one or more cameras (6, fig. 1) located at the premises and operatively coupled to the security gateway, and one or more audio stations (not shown) located at the premises and operatively connected to the security gateway, wherein the user is at a location which is geographically remote from the premises (figs. 1-3, page 6, line 3 to page 7, line 28).

Nabavi differs from claim 59 in that he does not teach the following: gateway provides an audiovisual signal at the premises for notifying an occupant at the premises that remote monitoring is occurring; security system provides for streaming data in substantially real time from the security gateway to the remote client, the security system provides for substantially real-time synchronized audio and video communication between the remote client and security gateway; security system provides the remote client with authorization information on a permission profile associated with the user.

However, Horii teaches the following: gateway provides an audiovisual signal at the premises for notifying an occupant at the premises that remote monitoring is occurring (fig. 1, see abstract); Lemons teaches the following: security system provides for streaming data in substantially real time from the security gateway (reads on 14, figs. 1, 4) to the remote client, the security system provides for substantially real-time synchronized audio and video communication between the remote client and security gateway (col. 3 lines 15-16); Nadooshan teaches the following: security system provides the remote client with authorization information on a permission profile associated with the user (figs. 5-6, 9, col. 6 lines 29-58; col. 7, line 48 – col. 8, line 14).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify Nabavi's system to provide for the following: gateway provides an audiovisual signal at the premises for notifying an occupant at the premises that remote monitoring is occurring as this arrangement would address the privacy concerns of user being observed as taught by Horii, thus safeguarding privacy concerns of users; security system provides for streaming data in substantially real time from the security gateway to the remote client, the security system provides for substantially real-time synchronized audio and video communication between the remote client and security gateway as this arrangement would facilitate to obtain real time data from monitoring premises as taught by Lemons, thus facilitating actual monitoring of the premises in real time; security system provides the remote client with authorization information on a permission profile associated with the user as this arrangement would provide means for centralized control of security access to the remote premises,

thereby enabling central control of access to remote systems as taught by Nadooshan which facilitates streamlining the security procedure for remote access.

5. Claim 60 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nabavi in view of Nadooshan.

Regarding claim 60, Nabavi discloses a method for remote monitoring of a premises, the method comprising: operatively coupling a remote client (9, fig. 1) to a security system server (reads on 10, fig. 1), the security system server being capable of authenticating a user of the remote client, operatively coupling the remote client the security gateway (reads on 1, fig. 1), the security gateway being capable of managing the monitoring of one or more premises of the premises using a plurality of devices operatively coupled thereto as shown in fig. 1, transferring information between the security gateway and the remote client, wherein the user is at a location which is geographically remote from the premises (figs. 1-3, page 6, line 3 to page 7, line 28).

Nabavi differs from claim 60 in that he does not teach the following: remote client cannot access the security gateway without the authorization information provided, to the remote client, by the security system server, wherein the information transferred between the security gateway and the remote client relates to selected ones of the plurality of devices for which the access permission identifies as devices that the user may access, and wherein the remote client can access the selected one of the plurality of devices but is prevented from accessing unselected ones of the plurality of devices.

However, Nadooshan teaches the following: remote client cannot access the security gateway without the authorization information provided, to the remote client, by

the security system server, wherein the information transferred between the security gateway and the remote client relates to selected ones of the plurality of devices (col. 4 lines 19-25) for which the access permission (reads on login level) identifies as devices that the user may access, and wherein the remote client can access the selected one of the plurality of devices but is prevented from accessing unselected ones of the plurality of devices (figs. 5-6, col. 6 lines 29-58; and fig. 9).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify Nabavi's system to provide for the following: remote client cannot access the security gateway without the authorization information provided, to the remote client, by the security system server, wherein the information transferred between the security gateway and the remote client relates to selected ones of the plurality of devices for which the access permission identifies as devices that the user may access, and wherein the remote client can access the selected one of the plurality of devices but is prevented from accessing unselected ones of the plurality of devices as this arrangement would facilitate to set up user access to different equipments and its features by setting up user login levels as taught by Nadooshan, thus satisfying different security needs required for given application.

6. Claim 61 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nabavi in view of Nadooshan and Katz.

Regarding claim 61, Nabavi discloses a method for remote monitoring of a premises comprising: operatively coupling a remote client (9, fig. 1) to a security system server (reads on 10, fig. 1), the security system server being capable of authenticating a

user of the remote client, operatively coupling the remote client to the security gateway (reads on 1, fig. 1), the security gateway being capable of managing one or more portions of the premises, transferring information between the security gateway and the remote client, wherein user is at a location which is geographically remote from the premises (figs. 1-3, page 3, line 3 to page 7, line 28).

Nabavi differs from claim 61 in that he does not teach the following: upon authentication of the remote client, the security system server transmitting, to the remote client, authorization information necessary for the remote client to access a security gateway for the premises, the remote client transmitting, to the security gateway, the authorization information transmitted to the remote client by the security system server, wherein the remote client cannot access the security gateway without the authorization information provided, to the remote client by the security system server; activating a signal at the premises for notifying an occupant at the premises that remote monitoring is occurring.

However, Nadooshan teaches the following: upon authentication of the remote client, the security system server transmitting, to the remote client, authorization information necessary for the remote client to access a security gateway for the premises, the remote client transmitting, to the security gateway, the authorization information transmitted to the remote client by the security system server, wherein the remote client cannot access the security gateway without the authorization information provided, to the remote client by the security system server (fig. 1, col. 4 lines 2-31; and

fig. 9); Katz teaches the following: activating a signal at the premises for notifying an occupant at the premises that remote monitoring is occurring (col. 10 lines 46-58).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify Nabavi's system to provide for the following: upon authentication of the remote client, the security system server transmitting, to the remote client, authorization information necessary for the remote client to access a security gateway for the premises, the remote client transmitting, to the security gateway, the authorization information transmitted to the remote client by the security system server, wherein the remote client cannot access the security gateway without the authorization information provided, to the remote client by the security system server as this arrangement would provide means for centralized control of security access to the remote premises, thereby enabling central control of all access to the remote systems as taught by Nadooshan; activating a signal at the premises for notifying an occupant at the premises that remote monitoring is occurring as this arrangement would provide initial notification to the affected users of the system who are being video recorded so that any privacy concerns are addressed before commencement of recording as taught by Kastz.

7. Claims 62-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nabavi in view of Nadooshan as applied to claim 60 above, and further in view of Lemons and Vanska et al. (US 2004/0172396A1, filed 5-17-2001, hereinafter Vanska).

The combination differs from claims 62, 63-64, 66 in that it does not teach the following: selected one of plurality of devices operably coupled to the security gateway

are life style monitoring devices and the unselected one of the plurality of devices operably coupled to the security gateway are not life style monitoring devices, the plurality of devices operably connected to the security gateway includes at least two video cameras/two audio stations, the life style monitoring devices include a first one of the at least two video cameras/two audio stations, and the non-life style monitoring devices include a second one of the at least two video cameras/two audio stations; general administrator of the security gateway, the access permissions to the user, the general administrator assigning the access permissions for the user such that user may only access lifestyle monitoring devices and is restricted from accessing devices which are not life style monitoring devices.

However, Lemons teaches the following: selected one of plurality of devices operably coupled to the security gateway are life style monitoring devices and the unselected one of the plurality of devices operably coupled to the security gateway are not life style monitoring devices, the plurality of devices operably connected to the security gateway includes at least two video cameras/two audio stations (fig. 4), the life style monitoring devices include a first one of the at least two video cameras/two audio stations, and the non-life style monitoring devices include a second one of the at least two video cameras/two audio stations (figs. 1, 4, col. 7 lines 26-65); and Vanska teaches the following: general administrator of the security gateway, the access permissions to the user, the general administrator assigning the access permissions for the user such that user may only access lifestyle monitoring devices (this reads on devices for which access rights are available) and is restricted from accessing devices

which are not life style monitoring devices (this reads on devices for which access rights are not allowed, fig. 3, paragraphs 0052-53).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: selected one of plurality of devices operably coupled to the security gateway are life style monitoring devices and the unselected one of the plurality of devices operably coupled to the security gateway are not life style monitoring devices, the plurality of devices operably connected to the security gateway includes at least two video cameras/two audio stations, the life style monitoring devices include a first one of the at least two video cameras/two audio stations, and the non-life style monitoring devices include a second one of the at least two video cameras/two audio stations as this arrangement would provide means for monitoring various spaces in user premises as taught by Lemons; general administrator of the security gateway, the access permissions to the user, the general administrator assigning the access permissions for the user such that user may only access lifestyle monitoring devices and is restricted from accessing devices which are not life style monitoring devices as this arrangement would provide means for selectively granting permission to certain equipment for controlling/monitoring purposes based on permission profile set up for each equipment/device as taught by Vansaka

Regarding claims 67-71, 72-75, they are rejected for the same reasons as set forth in the rejection of claims 60, 62-66.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Melur Ramakrishnaiah whose telephone number is (571)272-8098. The examiner can normally be reached on 9 Hr schedule.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Curt Kuntz can be reached on (571) 272-7499. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Melur Ramakrishnaiah
Primary Examiner
Art Unit 2643